ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ШИФРОВАНИЯ ИНФОРМАЦИИ

Хамутскиих Е.Ю.

ФГБОУ ВПО «Магнитогорский государственный технический университет имени Г.И.Носова», г. Магнитогорск, Россия

Необходимость технических средств защиты диктуется тем, что интернет – это источник информации, за который никто не несет ответственность, и вероятность получения из него недостоверной, оскорбительной, пиратской или запрещенной по другим причинам информации весьма велика.

Ключевые слова: криптография, шифрование, электронные ключи, информация, криптостойкость.

The need for technological protection measures dictated by the fact that the Internet – a source of information for which no one is responsible, and the probability of getting out of it inaccurate, abusive, pirated or illegal for other reasons information is very high.

Шифрование – это способ изменения сообщения или другого документа, обеспечивающее искажение (сокрытие) его содержимого. (Кодирование – это преобразование обычного, понятного, текста в код. При этом подразумевается, что существует взаимно однозначное соответствие между символами текста (данных, чисел, слов) и символьного кода – в этом принципиальное отличие кодирования от шифрования. Часто кодирование и шифрование считают одним и тем же, забывая о том, что для восстановления закодированного сообщения достаточно знать правило подстановки (замены). Для восстановления же зашифрованного сообщения помимо знания правил шифрования требуется и ключ к шифру. Ключ понимается нами как конкретное секретное состояние параметров алгоритмов шифрования и дешифрования. Знание ключа дает возможность прочтения секретного сообщения. Впрочем, далеко не всегда незнание ключа гарантирует, что сообщение не сможет прочесть посторонний человек.) Шифровать можно не только текст, но и различные компьютерные файлы – от файлов баз данных и текстовых процессоров до файлов изображений.

Шифрование используется человечеством с того самого момента, как появилась первая секретная информация, т. е. такая, доступ к которой должен быть ограничен.

Идея шифрования состоит в предотвращении просмотра истинного содержания сообщения (текста, файла и т.п.) теми, у кого нет средств его дешифрования. А прочесть файл сможет лишь тот, кто сможет его дешифровать.

Большинство из нас постоянно используют шифрование, хотя и не всегда знают об этом. Если у вас установлена операционная система Microsoft, то знайте, что Windows хранит о вас (как минимум) следующую секретную информацию:

- пароли для доступа к сетевым ресурсам (домен, принтер, компьютеры в сети и т.п.);
- пароли для доступа в интернет с помощью DialUp;

• кэш пароли (в браузере есть такая функция – кэшировать пароли, и Windows сохраняет все когда-либо вводимые вами в интернете пароли);

• сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере.

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

Криптосистемы разделяются на ***симметричные*** и ***с открытым ключом*** (или асимметрические).

В ***симметричных криптосистемах*** и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с ***открытым ключом*** используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины ***распределение ключей и управление ключами*** относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

– количество всех возможных ключей;

– среднее время, необходимое для криптоанализа.

Преобразование T_k определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования в целях защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста,

– должно быть не меньше общего числа возможных ключей;

– число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

– знание алгоритма шифрования не должно влиять на надежность защиты; незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

– структурные элементы алгоритма шифрования должны быть неизменными;

• дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

• длина шифрованного текста должна быть равной длине исходного текста;

• не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

• любой ключ из множества возможных должен обеспечивать надежную защиту информации;

• алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Основные современные методы шифрования

Среди разнообразнейших способов шифровании можно выделить следующие основные методы:

• Алгоритмы замены или подстановки – символы исходного текста заменяются на символы другого (или того же) алфавита в соответствии с заранее определенной схемой, которая и будет ключом данного шифра. Отдельно этот метод в современных криптосистемах практически не используется из-за чрезвычайно низкой криптостойкости.

• Алгоритмы перестановки – символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом. Алгоритм перестановки сам по себе обладает низкой криптостойкостью, но входит в качестве элемента в очень многие современные криптосистемы.

• Алгоритмы гаммирования – символы исходного текста складываются с символами некой случайной последовательности. Самым распространенным примером считается шифрование файлов «имя пользователя.pwl», в которых операционная система Microsoft Windows 95 хранит пароли к сетевым ресурсам данного пользователя (пароли на вход в NT-серверы, пароли для DialUp-доступа в интернет и т.д.). Когда пользователь вводит свой пароль при входе в Windows 95, из него по алгоритму шифрования RC4 генерируется гамма (всегда одна и та же), применяемая для шифрования сетевых паролей. Простота подбора пароля обусловливается в данном случае тем, что Windows всегда предпочитает одну и ту же гамму.

• Алгоритмы, основанные на сложных математических преобразованиях исходного текста по некоторой формуле. Многие из них используют нерешенные математические задачи. Например, широко используемый в интернете алгоритм шифрования RSA, основан на свойствах простых чисел.

• Комбинированные методы. Последовательное шифрование исходного текста с помощью двух и более методов.

Вывод

В данной статье рассмотрены некоторые виды шифрования, в «чистом виде» они использовались раньше, а в наши дни они заложены практически в любой, даже самой сложной программе шифрования. Каждый из рассмотренных методов реализует собственный способ криптографической защиты информации и имеет собственные достоинства и недостатки, но их общей важнейшей характеристикой является стойкость. Под этим понимается минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, по стойкости шифра можно определить предельно допустимый объем информации, зашифрованной при использовании одного ключа. При выборе криптографического алгоритма для использования в конкретной разработке его стойкость является одним из определяющих факторов.

Все современные криптосистемы спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полным перебором по всему ключевому пространству, т.е. по всем возможным значениям ключа. Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

Приведем оценки стойкости рассмотренных выше методов шифрования. Моноалфавитная подстановка является наименее стойким шифром, так как при ее использовании сохраняются все статистические закономерности исходного текста. Уже при длине в 20–30 символов указанные закономерности проявляются в такой степени, что, как правило, позволяет вскрыть исходный текст. Поэтому такое шифрование считается пригодным только для закрывания паролей, коротких сигнальных сообщений и отдельных знаков.

Стойкость простой полиалфавитной подстановки (из подобных систем была рассмотрена подстановка по таблице Вижинера) оценивается значением $20n$, где n – число различных алфавитов, используемых для замены. При использовании таблицы Вижинера число различных алфавитов определяется числом букв в ключевом слове. Усложнение полиалфавитной подстановки существенно повышает ее стойкость.

Стойкость гаммирования однозначно определяется длиной периода гаммы. В настоящее время реальным становится использование бесконечной гаммы, при использовании которой теоретически стойкость зашифрованного текста также будет бесконечной.

Можно отметить, что для надежного закрытия больших массивов информации наиболее пригодны гаммирование и усложненные перестановки и подстановки.

При использовании комбинированных методов шифрования стойкость шифра равна произведению стойкостей отдельных методов. Поэтому комбинированное шифрование является наиболее надежным способом криптографического закрытия. Именно такой метод был положен в основу работы всех известных в настоящее время шифрующих аппаратов.

Алгоритм DES был утвержден еще более 20 лет назад, однако за это время компьютеры сделали немыслимый скачок в скорости вычислений, и сейчас не так уж трудно сломать этот алгоритм путем полного перебора всех возможных вариантов ключей (а в DES используется всего 8-байтный), что недавно казалось совершенно невозможным.

ГОСТ 28147-89 разработан еще спецслужбами Советского Союза, и он моложе DES всего на 10 лет; при разработке в него был заложен такой запас прочности, что данный ГОСТ является актуальным до сих пор.

Рассмотренные значения стойкости шифров являются потенциальными величинами. Они могут быть реализованы при строгом соблюдении правил использования криптографических средств защиты. Основными из этих правил являются: сохранение в тайне ключей, исключения дублирования (т.е. повторное шифрование одного и того же отрывка текста с использованием тех же ключей) и достаточно частая смена ключей.

Список использованных источников

1. *Cloud technology as a tool for organizing the learning process in the Russian universities [Internet portal]. URL: http://cyberleninka.ru/article/n/oblachnye-tehnologii-kak-instrument-organizatsii-uchebnogo-protsessa-v-rossiyskih-vuzah.*
2. *Oshurkov V.A., Makashova V.N. Mechanisms to optimize program management of IT-projects // Sbornik nauchnyh trudov SWORLD. – N 1. – S. 66–72.*
3. *What is SSL [Internet portal]. URL: https://www.globalsign.com/en/ssl-information-center/what-is-ssl/.*
4. *Storozheva E.V., Valeev A.S., Kruzhilina T.V., Sergeev A.N. Modeling of the process of formation of economic literacy of students in the structure of additional education university [Internet portal]. URL: http://elibrary.ru/item.asp?id = 18319444.*
5. *Content filtering [Internet portal]. URL: http://www.microtest.ru/it-infrastruktura/informacyonnaya-bezopasnost/1055/.*
6. *Chernova E.V. Competence of teachers in the field of ideology cyber extremism prevention among young people [Internet portal]. URL: http://www.rae.ru/fs/?section = content&op = show_article&article_id = 10001813.*